Like Adding Wings to the Tiger: Chinese Information War Theory and Practice

by Mr. Timothy L. Thomas, Foreign Military Studies Office, Fort Leavenworth, KS.

Introduction

During the past five years, numerous Chinese military and civilian scholars published significant articles or longer works on information war (IW) and related issues (networking, information theory, simulations, etc.). An analysis of their works yields several interesting results.[1] First, the Chinese feel a compelling need to develop a specific Chinese IW theory. This theory must be in accordance with Chinese culture, the economic and military situation in the country, the perceived threat, and Chinese military philosophy and terminology.

Second, Chinese IW theory is strongly influenced by Chinese military art. China is quickly integrating IW theory into its People's War concept, for example, a development ignored in the West but one with far-reaching strategic and operational implications. It is also considering the development of an independent "net force" branch of service (to supplement the navy, army and air force), and potentially looking at applying the 36 stratagems of war to IW methods. Third, Chinese military science dictates that IW be divided into sub-elements very different from those studied in the United States. These include the forms, nature, features, distinctions, principles, types, circles, and levels of IW. These subdivisions are similar to Russia's IW methodology, and result in diverse IW definitions and discussions as compared with those in the West .

While a theory of IW with Chinese characteristics is developing, turning theory into practice has proven more difficult. This is not unusual since China is still developing the civilian and military infrastructure to support their philosophy.[2] This article will highlight key aspects of the Chinese specific approach to IW. It will begin by discussing how the information age has affected China's attitude toward warfare and the specific Chinese historical factors affecting this interpretation. Next, Chinese IW definitions will be discussed, and the training courses and organizational structures to teach IW will be investigated. Finally, an examination will be made of China's interpretation of IW activities during the fight for Kosovo, and the most recent training exercises in its military regions that try to turn theory into reality.

IW with Chinese Characteristics

How has the information age affected China's attitude toward warfare? It is fair to say that the major change was a reevaluation of how to evaluate and conduct warfare. China realized that it couldn't threaten countries as a superpower might do with its current nuclear force, but something it can do with its IW force. For example, China can theoretically threaten U.S. financial stability through peacetime IW. Electrons lie at the heart of not only IW but also the worldwide economic boom associated with stock markets and e-commerce. The characteristics of information (global reach, speed of light transmission, nonlinear effects, inexhaustibility, multiple access, etc.) control the material and energy of warfare in a way that nuclear weapons cannot.[3] IW attempts to beat the enemy in terms of promptness, correctness, and sustainability,[4] and electrons are capable of reaching out and touching someone a long way away. It thus makes complete sense to put a significant effort into developing an information-based capability in both the civilian and military sense. From the Chinese point of view, IW is like adding wings to a tiger, making the latter more combat worthy than ever before.

Recent reports of hacker attacks on U.S. labs indicate that China is moving from theory to practice in security matters as well. The Washington Times reported on 3 August 2000 that hackers suspected of working for a Chinese government institute broke into a Los Alamos computer system and took large amounts of sensitive but unclassified information. Los Alamos spokesman Jim Danneskiold stated that "an enormous amount of Chinese activity hitting our green, open sites" occurs continuously.[5]

Targets of Chinese IW include information sources, channels, and destinations,[6] and C4I and electronic warfare assets. First attack objectives, some note, will be the computer networking system linking political, economic and military installations of a country as well as society in general; and the ability to control decision-making to hinder coordinated actions. This requires that both cognitive and information systems are hit.[7] This IW focus implies that not just soldiers will conduct warfare in the future, but civilians too. Some Chinese theorists have recommended organizing network special warfare detachments and computer experts to form a shock brigade of "network warriors" to accomplish this task. They will look for critical nodes and control centers on networks, and sabotage them.[8] Thus both computer experts and soldiers, a reflection of China's changing attitude, may conduct warfare.

IW has also forced Chinese experts to reconsider how to compute the correlation of forces. The Chinese believe that military strength can no longer be calculated using the number of armored divisions, air force wings, and aircraft carrier battle groups. In the information age, invisible forces such as computing capabilities, communications capacity, and system reliability must also be studied.[9]

A second reevaluation of warfare was more traditional in nature. It is an update of an old theory, yet is probably China's most far-reaching IW development. Chinese theorists believe that the capabilities and qualities of the information era enhance and breathe new life into Mao Zedung's theory of a People's War. Chinese IW specialist General Wang Pufeng first noted this condition in 1995.[10] Author Wei Jincheng followed up this thought in 1996, adding that a People's War with an IW context can be

> Carried out by hundreds of millions of people using open-type modern information systems. Because the traditional mode of industrial production has changed from centralization to dispersion, and commercial activities have expanded from urban areas to rural areas, the working method and mode of interaction in the original sense are increasingly information-based…the chance of the people taking the initiative and randomly participating in the war increased.[11]

Electronics, computer, and information engineering experts are as likely to become the genuine heroes of a new People's War much like the warrior class of the past, some believe.[12] Perhaps this focus explains why, in addition to economic factors, China is willing to reduce its army--China can "keep up" with other countries by utilizing a multitude of information engineers and citizens with laptops instead of just soldiers. China clearly has the people to conduct "take home battle," a reference to battle conducted with laptops at home that allow thousands of citizens to hack foreign computer systems when needed. China has a number of superior software writers and much untapped potential in the information field. As one author stated, if one or two per cent of any population has an IQ over 139, as studies predict, then China must have tens of millions of people in this category. The problem is how to find more information space and equipment for all of these people.[13]

IW specialist Shen Weiguang wrote that combatants can be soldiers or a teenager, whoever possesses the weapon called a computer. The whole of society will replace traditional battlefields, and different classes and social groups will take part in political activities of their own country or any country, in Shen's view. He advocated developing information protection troops, composed of scientists, police, soldiers, and other experts versed in IW, to safeguard the security of the national information boundary, and to launch counterattacks against an information invasion by other countries. [14] The goal of Chinese doctrine is to unify the concept of People's War with the concept of victory through information.[15]

Chinese analysts are keen to point out the increased role of society in foreign IW scenarios. Wang Xiaodong, while analyzing a RAND IW document, observed that this study unknowingly outlined a People's War in the information age. This was because the authors went back to the day before the IW assault to analyze what could have been done by society to protect them. He added

> Even as to government mobilized troops, the numbers and roles of traditional warriors will be sharply less than those of technical experts in all lines…since thousands of personal computers can be linked up to perform a common operation, to perform many tasks in place of a large-scale military computer, an IW victory will very likely be determined by which side can mobilize the most computer experts and part-time fans. That will be a real People's War…[16]

Ideas for uniting a People's War with IW are finding fertile ground in the 1.5 million-reserve force of China. The People's Liberation Army (PLA) is turning reserve forces in some districts into mini IW regiments. For example, in the Echeng District (about 700 miles due south of Beijing) in Hubei Province, the People's Armed Forces Department (PAFD) reportedly

organized 20 city departments (telecommunications, power, finance, TV, medical, and so on) into a militia/reserve IW regiment. The PAFD had a network warfare battalion, as well as electronic warfare (EW), intelligence, and psychological warfare (PSYWAR) battalions, and 35 technical "Fenduis" (squad to battalion). The PAFD also set up the first reserve IW training base for 500 people. Instructors at the base have reportedly run an "Informaticized People's Warfare Network Simulation Exercise." Even a web site was given for the Echeng District PAFD, http://ezarmy.net.[17]

On 27 June of 2000, the city of Ezhou (in the Echeng District of Hubei Province) carried out a national defense mobilization exercise via computer networks. The initial mission, according to Zhu Jianjian, commander of the military sub-district, was to explore how civil networks can be used in wartime and how networks can be used for rapid mobilization in order to improve the quality and efficiency of national defense mobilization work. A second mission was to recruit technical soldiers and scientific and technological equipment from the national defense mobilization database. An additional task was to establish wartime command organs, and to formulate various preliminary plans. During the exercise, networks of the command center and the member units of the city's national defense mobilization committee were linked to transmit audio and video information to each other. Cable TV and computer networks were integrated and put to use.[18]

Echeng is not the only district with reserve/militia units conducting IW training. The Fujan Province, according to a published report, held a meeting at Xiamen in December of 1999 that utilized reserve and militia forces. The report cited militia high-technology Fenduis that carried out electronic countermeasures, network attack and defense, and radar reconnaissance operations. These operations were conducted as part of an enforced blockade of an island. The Xiamen area is a special economic zone and attracts a higher than usual number of science and technology clients to the area.[19] Thus it is a prime area for IW related activities. There are also reports of reserve IW activity in Xian PAFD, and in the Datong military sub-district (MSD).

In Xian, the PAFD IW Fendui acted as OPFOR for a military district exercise in the Jinan Military Region. Ten IO methods were listed: planting information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; disseminating propaganda; applying information deception; releasing clone information; organizing information defense; and establishing network spy stations.[20] In Datong, 40 plus members of a high technology unit focused on information security, and on seizing partial "network domination" in network warfare. The unit held three network warfare OPFOR demonstrations for the Beijing Military Region, the Central Military Commission, the General Staff, and North China PLA units.[21]

In a special article in August 2000 entitled "PRC Army Pays Attention to the Role of Network Warfare," a People's War received as much attention as networking. The author stated that

> Some military figures noted that People's War has undergone an epochal leap from supporting the front army that made its advances on vehicles to contemporary network warfare "on keyboards…" Jiefangjun Bao [the Chinese Armed Forces newspaper] maintains that it is necessary to formulate rules and

> regulations regarding mobilization and preparation for "modern People's War" as well as information gathering and processing, online offensives and defenses, network technology research and exchanges, and so on in order to provide the norms for the orderly preparation and building of a "network People's War."[22]

A third and significant way that the information age has affected China's attitude toward warfare is that China's 36 stratagems may find new meaning and application. Some 300 years ago an unknown scholar decided to collect all of China's 36 stratagems and write them down. His work was called The Secret Art of War: The 36 Stratagems. The work emphasized deception as a military art that can achieve military objectives. In the information age, which is characterized by anonymous attacks and uncertainty (for example, the origin of viruses or the existence of back doors in programs, making anyone feel vulnerable), the stratagem just might be revitalized as a tactic. It should be easier to deceive or inflict perception management injuries ("guidance injuries" in Chinese) as a result. The information age is developing into the age of anonymous persuaders.

Some argue that in today's high tech world, these ancient stratagems are no longer applicable. However, a look at just the first five stratagems demonstrates that this is not the case. Strategy one is "fool the emperor to cross the sea."[23] This means that in order to lower an enemy's guard you must act in the open hiding your true intentions under the guise of common every day activities. The IW application would be to use regular e-mail services or business links over the Internet to mask the insertion of malicious code or viruses. Strategy two is "besiege Wei to rescue Zhao." This means that when the enemy is too strong to attack directly, then attack something he holds dear. The IW application is that if you can't hit someone with nuclear weapons due to the catastrophic effects on your own country, then attack the servers and nets responsible for Western financial, power, political and other systems stability with electrons. Strategy three is "kill with a borrowed sword." This means that when you do not have the means to attack your enemy directly, then attack using the strength of another. The IW application is simple—send your viruses or malicious code through a cut out or another country. Strategy four is "await the exhausted enemy at your ease." This means that it is an advantage to choose the time and place for battle. Encourage your enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, you attack with energy and purpose. The IW application here is to use the People's War theory to send out multiple attacks while saving the significant attack for the time when all of the West's computer emergency response teams (CERT) are engaged. Finally strategy five is "loot a burning house." This means that when a country is beset by internal conflicts, then it will be unable to deal with an outside threat. The IW application is to put hackers inside the West (under the guise of a student or business) and attack from the inside. While chaos reigns, steal from information resource bases.

A May 2000 Chinese article on Internet War offered the implied logic behind "why" military leaders might use such stratagems today. The article stated that China is a relatively weak information operations power at the moment and must use tricks and strategy as an invisible combat strength to make up for the shortage of material conditions.[24]

A fourth characteristic affecting China's attitude toward warfare is the focus on knowledge warfare as a competitor to IW. Knowledge warfare refers to a battle of competing brains

(decision-makers on both sides of a confrontation) that process seemingly endless streams of information (the IW connection) and regurgitates the information in intelligible, useable form giving one side an advantage. Innovation and the ability to "think outside the box" are also important. The speed of both innovation and processing thus determines combat power.[25] This implies that a commander must be able to think in terms other than two-dimensional maps, telephones, and so on. "How to think" may be more important than how to do something. Shen, for example, believes that the losers in future war will be those lacking command thinking rather than backward technology.[26] Thus the confrontation of two commands is a type of knowledge war that involves a trial of strength revolving around the procurement, control, and use of information,[27]making intellectual resources as important as scarce resources. Knowledge is becoming the paramount strategic resource, more important in the balance of power than weapons. Warfare thus may be waged around the struggle for intellectual resources, such as the allegiance of a hi-tech expert or the patented right to a piece of technology according to some.[28]

Finally, consideration is being given to developing a "net force," a separate branch to fight the high tech battles of the future. This is a significant development if it ever occurs (the article's authors stated that it was "very likely" to happen), as it will represent a dramatic break from the old construct of a navy, army and air force as the main branches of the armed forces. The Chinese believe that violations of cyberspace are as important (if not more so due to their concealed nature) than violations of national sovereignty, especially if vital information resources or data banks are penetrated and information stolen.[29] Thus, a net force is needed.

The net force would protect net sovereignty and engage in net warfare, a technology and knowledge-intensive type of warfare. Net technology would include scanning technology to break codes, steal data, and take recovery (anti-follow-up) actions. It would include superior offensive technology capable of launching attacks and countermeasures on the net, including information-paralyzing software, information-blocking software, and information-deception software. It would include masquerade technology capable of stealing authority from the network by assuming a false identity. And it would include defensive technology that can ward off attacks, serve as an electronic gate to prevent internal leaks, and block arbitrary actions much like an electronic policeman.[30]

There are also several terms that are found only in Chinese writings that add to the idea of IW with Chinese characteristics. These include military soft science[31] ; information frontier, information alliance, information factory, information police, and informationized army[32]; deceptive, occupation/hindrance, contamination, blocking, and guidance injuries[33]; negative entropy, information volume, information quality[34]; information invasion, information deterrence, information protection troops[35]; and informationized war and information assault.[36]

Chinese IW Definitions: Focus on Network and Cognitive Processes

[[For comparative purposes for the remainder of this section, the U.S. armed forces definitions of information operations and information war are presented here: Information operations "are actions taken to affect adversary information and information systems, while defending one's

own information and information systems. …major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA."[37] Information war is "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[38]]]

There are several Chinese authors who command respect for the scope of their works and depth of their thought on IW issues. Dr. Shen Weiguang, Major General Wang Pufeng, Senior Colonel Wang Baocun, and General YuanBanggen are certainly among these individuals, if not at the top of the list.

Studying Chinese IW definitions consecutively by year offers clues to the developing nature of Chinese IW theory.The definition of IW offered by Shen Weiguang in 1996, one of the first, stated that IW is a war in which both sides strive to hold the battlefield initiative by controlling the flow of information and intelligence. This initial definition did not address information superiority or information operations, just control. Instead of protecting friendly information systems and attacking enemy systems, as the U.S. defines the term, Shen emphasized protecting oneself and controlling the enemy. [39] Wang Pufeng, also writing in 1996, stated that the central issue in achieving victory in IW is control of information. Authors Yang and Guo added their voices to this emphasis on control, stating that the most important initiative on future battlefields would be the power to control information. Victory will be determined by the side that has the capability to control information resources and their utilization. These are the indices of a nation's capacity to direct a war effort, they wrote.[40] Thus in 1996 the emphasis was clearly on control.

In 1997 there were fewer attempts to define IW. Author Liang Zhenxing stated that IW includes all types of war fighting activities that involve the exploitation, alteration, and paralysis of the enemy's information and information systems, as well as all those types of activities which involve protecting one's own information and information systems from exploitation, alteration, and paralysis by the enemy. Liang added that the Chinese definition of IW should take cognizance of Chinese characteristics but be in line with the definition prevailing internationally. Perhaps for that reason his IW definition is closer than some to the U.S. definition. Liang added that the essence of IW is to render the operational space unclear and indistinct to the enemy while making it transparent to one's own forces.[41] Another 1997 author, Wang Baocun, provided a masterful description of IW through the dissecting eyes of Chinese military science. His article covered the forms, nature, levels, distinctions, features and principles of IW. He listed forms of IW as peacetime, crisis and wartime; the nature of IW as reflected in offensive and defensive operations; levels of IW as national, strategic, theater, and tactical; and other distinctions of IW as command and control, intelligence, electronic, psychological, cyberspace, hackers, virtual, economic, strategy and precision. He listed features of IW as complexity, limited goals, short duration, less damage, larger battle space and less troop density, transparency, the intense struggle for information superiority, increased integration, increased demand on command, new aspects of massing forces, and the fact that effective strength may not be the main target. He stated that principles of IWinclude decapitation, blinding, transparency, quick response, and survival.[42] His definition and analysis offer some of the most important insights into Chinese IW.

In 1998 there were even fewer original discussions of the term IW. One analyst defined IW as the ability to hinder an opponent's decision-making while protecting friendly decision-making abilities. It is interesting that the Chinese emphasis is not on attacking enemy information or information systems but on "hindering" an opponent's decision-making.[43] It is a slight but significant diversion from the U.S. definition.

In 1999 Chinese analysts again returned to a serious debate over IW issues. Shen Weiguang defined IW this time more broadly as involving two sides in pitched battle against one another in the political, economic, cultural, scientific, social, and technological fields. The fight was over information space and resources. He also defined IW narrowly as the confrontation of warring parties in the field of information. The essence of IW, Shen wrote, is to attain the objective of "forcing enemy troops to surrender without a fight" through the use of information superiority.[44] Obviously this definition echoes historical Chinese thoughts on warfare. However, this seems to imply that information superiority is more of a cognitive than systems related process.

Another Chinese author who defined IW in 1999 was Yuan Banggen, the head of a General Staff Directorate. He stated that IW is the struggle waged to seize and keep control over information, and the struggle between belligerent parties to seize the initiative in acquiring, controlling and using information. This is accomplished by capitalizing on and sabotaging the enemy's information resources, information system, and informationized weapon systems, and by utilizing and protecting one's own information resources, information systems, and informationized weapon systems. Yuan thus substitutes capitalizing and sabotaging for the U.S. term attacking while simultaneously emphasizing control. He also noted that IW is a kind of knowledge warfare (see above), a rivalry between groups of professionals with hi-tech knowledge.[45]

Senior Colonel Wang Baocun, the author who did such a good job of dividing IW into its various components in 1997, offered a third 1999 IW discussion. He distinguished between IW and informationized war, defining IW as a form of fighting and part of a complete war, and informationized warfare as an entirely new form of war. IW will gradually become informationized war, Wang noted, but this won't happen until the middle of the 21st Century when informationized forces will be available. The latter is the follow-on to mechanized forces. Wang views informationized forces as the soul of Sun Tsu's "subduing the enemy without battle," a tactic requiring superior military strength, full preparedness, destroying the enemy's strategy, and cultivating, conducting and fostering discipline. The goal is to "force the enemy side to regard their goal as our goal," to "force the opponent to give up the will to resist and end the confrontation and stop fighting by attacking an enemy's perception and belief via information energy." If perceptions are attacked correctly, morale drops and with it control, the main ingredient in IW.The proper information assault can make this work.[46] Wang's discussion thus includes some cognitive aspects of IW and again an emphasis on control.

Xie Guang, the Vice-Minister of the Commission of Science, technology and Industry for National Defense, also defined IW in late December 1999.He stated that IW "in the military sense means overall use of various types of information techniques, equipment, and systems, using disturbance, misinformation or destruction of the enemy's information systems,

particularly his command systems, to shake the determination of the enemy's policymakers, and at the same time the use of all means possible to ensure that one's own information systems are not damaged or disturbed."[47]China's external IW goal is thus to shake the determination of opposing policymakers, while its internal goal is to protect information systems. Xie also described the three areas of IW as first, command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), second electronic warfare, and third computer attack and defense methods.

Finally, in 2000, IW specialist Wang Pufeng offered a deeper explanation of information war than any seen to date, distinguishing it from information warfare. In Wang's opinion, an information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and a kind of operational pattern. The new operational pattern refers to operations in a computer network space. Information warfare embraces information detection systems, information transmission systems, information and weapon strike systems, and information processing and use systems. IW embraces information warfare. Both integrate information and energy and use an information-network-based battlefield as their arena of activity.[48]

There were very few Chinese authors who attempted to define information operations, a subject touched on by Wang Pufeng. One who did was Yuan Banggen in his 1999 article. He stated that information operations (IO) are specific IW operations. IW is the core of informationized warfare, whereas information operations are the manifestation of information warfare on the battlefield, in Yuan's opinion. IO means information wars in the narrow sense, that is the military field, and they are usually integrated, high and new technology countermeasures. IO's theoretical system is formed from two levels, basic and application. Basic theories consist of basic concepts about IO, its organizational structure and technological equipment, command and control for IO, and so on. Application theories can be categorized into offensive IO and defensive IO, strategic, operational, campaign and tactical levels, and into peacetime, wartime, and crisis-period IO. All activities of IO center on command and control. IO's two missions are preparation and implementation. Its principles are centralized command, multi-level power delegation, multi-dimensional inspection and testing, timely decision-making, and the integration of military and civilian actions with a focus on key links.[49]

Yuan also discussed digital forces and digital battlefields in the same article. Digital forces are new-generation combat units. These forces are mainly armed with digitized electronic information equipment and combat weapons. They are characterized by the integration of command and control, intelligence, reconnaissance, early warning, detection, communications, and electronic countermeasures and by the intellectualization of principal combat weapons.The digital battlefield denotes the battlefield where the effective linking and use of strategic, campaign, and tactical command automation systems are realized, based on digital information technology. Digital forces and digital battlefields are the two main components of IW. Digital forces can also be called informationized forces and digital battlefields can also be called informationized battlefields.[50] The digitization standard of the communication system affects and determines the quality and process of the construction of digital forces and digital battlefields. Therefore, the construction of the digitized communication system is the "core of cores" in the construction of digital forces and digital battlefields.[51]

One author briefly discussed what he called information network warfare (INW). He broadly defined it as a war in which two opposing sides try to take over information space and vie for information resources. Narrowly defined an INW refers to a confrontation on the network between two opposing sides in war. INW tests human willpower, intelligence, and technology.[52]Author Qi Jianguo suggested uniting the network with a People's War. He recommended that the PLA establish an authoritative, centralized and united network People's War organizational organ. It would control information operations and networking activities, and allow for the conduct of mobilization exercises and education on People's War on the net. Similar organs would be established at different levels in the provinces, cities, and prefectures. Laws and regulations need to be formulated in order to standardize the preparations and development of a network People's War.[53] It was noted that China must uphold the principle of combining the establishment of networks for both wartime and peacetime use, setting up networks for both military and civilian use, and develop Internet service in a limited manner.[54]

While most of the definitions above focused principally on systems, there is also a Chinese predilection to study cognitive processes. In fact some, like Shen, believe that IW's essence is the sum of information capabilities capable of breaking the enemy's will to resist by attacking his cognitive understanding and convictions causing the enemy to give up all resistance and terminate the war. The main tasks of IW are disrupting the enemy's cognitive system and trust system, Shen noted in 1996.[55]

Wang Baocun also believes strongly in the union of IW and cognitive processes. He described perception structures, perception systems, and belief systems as IW components in one of his articles. He defined a perception structure as "all things that an individual or a group considers correct or true, regardless of whether these things that are considered correct or true have been obtained through perception or belief." Perception structures are defined as composed of perception systems, those "systems which are established and operated in order to understand or observe verifiable phenomena by turning such phenomena into perceptible realities and subsequently to make decisions or take action on the basis of intuitive understanding of such realities."Belief systems are "systems which guide testable empirical information and such information and consciousness that cannot be tested or are hard to test."[56]

This focus on perceptions and beliefs is interesting because some Chinese IW specialists believe that communications and the media are the main areas of IW concern today. According to Yang Minqing, IW is a face off in the field of information between opposing parties. This is reflected primarily in a fight to gain the initiative over information resources and control of the production, transmission, and processing of information so as to damage information-based public opinion on the enemy's side. Yang believes that IW is divided into two fields. They are national IW (which tries to seize information by intelligence, diplomacy, commercial, and strategic psychological warfare) and national defense IW (which tries to maintain an upper hand over information acquisition between two armies, and includes intelligence, electronic, command and control, and psychological warfare). In both cases the fight is over information space and information resources. A point of IW concern is communications/media, which can play a strategic role. Communications can also have a deterrent effect, and possess an ability to manipulate the populace, wherein lies its importance as a target.[57]

Chinese Organizations and Training to Conduct IW

There are several organizations charged with IW instruction for the PLA. The lead organization is the Communications Command Academy. The Academy is located in Wuhan, the capital of central China's Hubei Province. In 1998 the Academy announced the publication of two books, Command and Control in IW and Technology in IW that became the leading Chinese IW texts. The first book discussed who should exercise command and control (C2), the means to exercise C2, the spheres, principles and forms of IO, new concepts for building an information corps, and the principles on which IW should be based. The second book explored the composition, characteristics, and development trends of basic IW technologies. This included the retrieval, transmission and processing of information. It also established a structural system for IW and offered strategies for technological developments in the army. The Academy is well respected for its IW curriculum that analyzes strategic, operational, and tactical IW requirements.[58] Nearly two years later, the Communications Command Academy hosted a training course on information war, research on information command and tactics, and research on information combat.[59] Interestingly, the academy is located not far from the reserve component IW regiment in Echeng district.

A second leading PLA IW institute is the Information Engineering University, established by combining the Institute of Information Engineering, the Electronic Technology College, and the Survey and Mapping college. The university is located in Zhengzhou, the capital of Henan Province. It will help cultivate professionals for hi-tech warfare involving the use of information, according to President Major General Zhou Rongting, and will create a number of new specialties such as remote image information engineering, satellite-navigation and positioning engineering, and map data banks. Major specialties include information security, modern communications technology, and space technology.[60]

A third PLA IW location is the Science and Engineering University. It was established by combining the Institute of Communications Engineering, the Engineering Institute of the Engineering Corps, the Meteorology Institute of the Air Force, and the 63rd Research Institute of the General Staff headquarters. It trains new military personnel in fields such as IW, communication and command automation, and other subjects.[61] University President Major General Si Laiyi said that a new Institute of Computer and Command Automation set up six disciplines, including electronic engineering, information engineering, network engineering, command automation engineering, and counter-information with key information warfare technologies as the core. There are over 400 experts and professors at the university teaching IW theories and technological subjects.[62]

A fourth PLA IW institute is the National Defense Science and Technology University in Changsha.Directly under the supervision of the Central Military Commission, it is where the "Yin He" series of supercomputers are developed.[63] From April to June of 1999 some 60 senior officers (average age 53) studied hi-tech warfare at the university while the war over Kosovo was raging.Lessons included reconnaissance, monitoring technology, precision guidance technology, electronic war, and information war, among other subjects. One conclusion about future wars was that "an information umbrella has become the most important factor, and the opponent's nerve center the most important military target."[64] The university apparently runs

this course several times a year at army level and at levels above army.[65] The most recent class was held in April 2000. Nearly 300 officers had received training at the university by that time. Special emphasis in the most recent class was placed on instruction and discussion of electronic and information techniques (and associated topics, such as guidance control, command automation, etc.) and "three offenses and three defenses" training (see discussion below on this latter subject).[66]

A PLA Navy institute studying IW is the Navy Engineering College headed by President Shao Zijun. The general orientation of the College is to combine arms and information. Integrating electronic information with weapons systems does this. The College hopes to help adapt the Chinese Navy to the combat needs of information warfare. The College is also located in Wuhan and perhaps shares research on IW with the Communications Command Academy.[67]

These universities and colleges reflect the IW changes that the PLA foresees. Information is viewed as a multiplier of combat effectiveness and a strategic resource. In the opinion of some instructors, warfare is now about intelligence and resourcefulness, new temporal-spatial concepts, resolute decisiveness, and the "soft science" technology located in new weapons.[68] These forms and means present significant challenges to Chinese cadres assigned the job of teaching these subjects since the level of science and culture among commanders is relatively low. The system of training advanced in 1996 to handle this problem involved first laying a sound strategic foundation, then improving everyone's knowledge about IW by studying the experiences of foreign armies. These steps were to be followed by expanding basic IW skills, especially in electronic and psychological warfare, and in information attack and defense. Finally attention would be paid to converting knowledge to ability through the conduct of IW exercises. Press reports indicated that this plan was followed.[69] The first years were spent discussing the strategy and theory of the Revolution in Military Affairs and the use of IW in the Gulf War. A general discussion of the meaning and use of the offensive and defensive components of IW followed this. Finally, since 1997 numerous IW exercises were reported in the press.

One of the more interesting articles on IW training appeared in February of 1999. IW was defined as knowledge-style warfare, a special trial of strength between highly talented people. This definition arose from the fact that hi-tech war demands a high level of knowledge by commanders and operators, strong psychological qualities, command ability, and operational skills. Recognizing that China lags behind in several of these categories, the PLA leadership has decided to carry out training at various levels. Each is age dependent. The first category is support-style talent, where the main targets are leading cadres who are over 40 years of age. These are decision-makers, and the aim is to eliminate their information illiteracy, to change their concepts through training (from mechanized concepts to simulated IW fighting), and to apply their new ideas to future war. Training content for this group is information technology basics, the theory of IW, and general knowledge of IW weapons. Method of training is to focus on short training courses, supplemented by other methods.[70]

The second category is transitional-style talent. Here cadres aged 30-40 were targeted. As the future leaders of China, they must focus on enhancing their ability to command in IW environments. Training aims were to supply them with information technology lessons they may have missed in college, and to ensure they grasped the requirements, special features, and laws of

future IW. It was also important for them to understand the components of information weapons systems, and to have instructors lay a firm foundation for information theory. Finally, they must master the principles, forms, methods, and skills for IW command.[71]

The third and final category is called regeneration-style talent. This involved cadres aged 30 or less. These individuals are already acclimated to information society and possess a general all-round foundation in modern information technology theory. Their focus is on both command and technology. They receive advanced IW training, from ideological concept to theoretical foundation to skill in application. As opposed to the other two age groups, their training method is long.[72]

The training for each age group includes:

- basic theory, including computer basics and application, communications network technology, the information highway, and digitized units
- electronic countermeasures, radar technology
- IW rules and regulations
- IW strategy and tactics
- theater and strategic IW
- information systems, including gathering, handling, disseminating, and using information
- combat command, monitoring, decision-making, and control systems
- information weapons, including concepts, principles of soft and hard destruction, and how to apply these weapons
- and simulated IW, protection of information systems, computer virus attacks and counterattacks, and jamming and counterjamming of communications networks.[73]

This article made it appear that China is well on its way to developing a first rate IW curriculum. But later reports suggest that this is still wishful thinking. For example, a July 1999 report noted the following:

> Irrationalities in the training content, system, and structure have kept IW training from truly becoming the mainstream of our military training. At present, IW training is in a "do-as-you-please" situation in which the content is not systematic, the operations lack order, there are no assessment standards, and management lacks regulations.[74]

The requirement to fulfill many of these points was reemphasized in October of 1999 by Fu Quanyou, chief of the Chinese General Staff. He wrote that four new aspects must be created. These were: create new IW theories, design a 21st century system of hi-tech military training, create high-tech military training forms and methods, and create operational, coordinating, and support training management mechanisms.[75]

A final item worthy of mention is the training style know as "striking at three things and defending against three things" which the Chinese claim has been upgraded to information age standards. Old style "three-three" was centered on exhausting the enemy's vital forces, preserving China's vital forces, and striving for superiority in manpower, firepower, and

machine power. The focal point of contention was to gain superiority in material capability. New style "three-three" is centered on obtaining, transmitting, handling, and protecting information, and the focal point of contention is to achieve information superiority."Striking at three things" means countering enemy destruction by active offensive means to ensure the stability of China's information system. It also means defending against precision attacks, and is designed to obtain target information. Units at and above army level should focus their study on reconnaissance and early warning, command coordination, and application of strategy. Divisions and brigades should focus on studying the application of firepower and the improvement and innovation of hardware. Units at and below regimental level should study and train in how to "respond rapidly and hit accurately."[76]

Defending against three things means obtaining optical, infrared, and electromagnetic target information. The key lies in adopting various means to seal off and weaken information on the target's external radiation, or make the enemy receive erroneous information. In addition, as students of the dialectic, Chinese military scientists view IW developments through a "thesis" and "anti-thesis" dialectical framework and concoct much of their training and research in a similar fashion. They recommend conducting various types of "anti" training, such as anti-reconnaissance, anti-cruise missile, and anti-interference training to offset IW weaponry. They think in terms of establishing an anti-information battlefield monopoly in order to offset another nation's information superiority.

Chinese Perceptions of the IW Battle for Kosovo

Chinese IW specialist Wang Baocun offered the best analysis of how both the Serbian Armed Forces and NATO used IW during the conflict. Defining IW as "a military struggle in the information arena for the power to create information," he discussed NATO's offensive IW and Serbian defensive IW.[77]

NATO used IW in the pre-conflict stage, according to Wang, through extensive reconnaissance and monitoring of the potential conflict area. This included the use of military satellites, reconnaissance, electronic monitoring and what Wang described as the use of 400 spies. NATO began the next phase of the operation, the strike stage, by "beheading" the Yugoslav army's command system through a series of strikes. NATO then used IW superiority in the air (MiG-29's do not have advanced electronic information systems to safeguard it) and waged an effective air war. At the same time, electronic warfare capabilities focused on assessing battle damage swung into high gear. Thus from Wang's point of view, the NATO strike engagement package included electronic countermeasures, precision strikes, and damage assessment. Simultaneously a variety of psychological warfare means were employed. Wang defined psychological warfare as "offensive warfare" aimed at changing the mental state of the enemy army and people. NATO first intensified the protection of its own information and prevented third parties from providing intelligence information to the FRY. Wang reported on the creation of a NATO information blockade that prevented the Yugoslav army and people from obtaining key information.[78]

Protective measures taken by NATO were well advised and paid dividends. The Chinese Liberation Army Daily (LAD) disclosed on 27 July 1999 that a "network battle" was fought

between Chinese and U.S. hackers following the 8 May bombing of the Chinese embassy. U.S. hackers, according to the report, aimed their counterattack at the following web sites:

- Xin Lang Wang or Sina— http://home.sina.com.cn
- Zhongwen Re Xun or Yesite—http://www.yesite.com
- Shanghai Wang Sheng or Shanghai Web Boom (no http listed)

The Chinese initiated the U.S. hack by altering the home page of the U.S. Embassy in Beijing, writing on it"down with the Barbarians." The Chinese also report causing a blackout at a few U.S. political and military web sites, and some 300 civilian web sites. The methodology for performing these hacks, according to the LAD article, was the mobilization of thousands and thousands of net users to issue a ping command to certain web sites at the same time. This caused servers to be overloaded, and paralyzed these websites. In addition, thousands and thousands of e-mails were sent daily to the opposite side, thus blocking mail servers. Viruses were sent via e-mail, and attacks were launched with "hacker tools" hidden in certain programs. The LAD article called for developing a computer network warfare capability, training a large number of network fighters in PLA academies, strengthening network defenses in China, and absorbing a number of civilian computer masters to take part in actions of a future network war.[79]

Wang had high praise for the IW countermeasures utilized by Serb forces against NATO air attacks.The primary countermeasure was to use concealment to preserve Serb military strength. They did this by hiding planes in caves and along ring roads and highways; hiding armored vehicles in forests, near buildings in cities, and in mountains; allowing the army to disperse in cities and villages, mingling with the Albanians; and moving command and control organizations underground. They also used technical means to avoid enemy reconnaissance. These measures included not switching on air defense radar, calculating when military satellites would go over, putting greenery on armored vehicles or placing them next to heat sources, displaying corrugated iron and other radar "bait" to attract missiles and planes ("conceal the genuine and display the fake"), and taking advantage of weak points (such as the fact that surveillance cannot pierce smoke and clouds).Finally, like China, the Serbs used the Internet to fight NATO. They set up a number of sites on the worldwide web to describe how NATO was carrying out its air strikes, and tried to overload NATO systems with excessive numbers of e-mail.[80]

A Chinese analyst noted that as the earth shrinks in virtual size via the use of information technology (telecommunications, the Internet, etc.), the size of the battlefield is actually growing. This includes, of course, all of the key nodes making up our virtual networks.The Chinese call attacks on key nodes "acupuncture war," with key points on the network become targets. Net points are of crucial importance to the survivability of a network. According to Metcalfe's Law "the value of a network is the square of the number of net points." So by destroying net points one gets twice the results with half the effort in geometric terms. In addition to net point warfare, the Serbs learned valuable lessons from what the Chinese termed the "three anti's and one resistance." The three antis included anti-reconnaissance, anti-interference, and anti-invisibility, and the resistance was working against destruction. The Chinese armed forces also noted that militaries must change from organizing according to weapon systems to organizing according to

information systems. The Chinese military must become flexible, more like "building blocks" that can be quickly restructured and reorganized.[81]

One article suggested that the Kosovo conflict was an example of the U.S.'s application of asymmetrical warfare. The latter was defined as "war between forces of different types, such as air force to navy, air force to army, navy to army, or army to air force." The key to asymmetrical warfare is to bring respective service advantages into full play, to pit the superior against the inferior and to avoid strengths while attacking weaknesses. Interestingly, the author quoted Mao Zedong at this point, who suggested that many armies were against going head to head with other armies. As a counter, Mao believed that "we are not like Sung Hsiang-kung, not being so stupidly humane, just and virtuous." This belief certainly puts a different slant on asymmetry, sounding more like the book by two PLA colonels entitled Unrestricted War! Asymmetrical war was further described as having smart war characteristics, such as being grounded in technology, having information as its mainstay, developing in the direction of no-contact warfare, and making the battlefield more multidimensional. While this description of asymmetrical warfare is an over exaggeration of the concept, it nonetheless reflects how some Chinese interpret it.[82]

Another article discussed NATO's information monopoly on the asymmetric battlefield. This meant that NATO could choose the forces, time and space it wanted to apply combat power on the battlefield, allowing one side to control a larger battlefield radius than the other. The understanding is that one side's antenna or feelers can reach out farther than the other, enabling it to engage in no-contact or "beyond-defense" warfare. This ability offered absolute control of the situation. As a counter, the Chinese recommended developing anti-information, anti-air, and anti-battlefield monopolies. The article suggested that in order to overcome these monopolies China must "change our ideas, creating new battlefields such as the special operations battlefield, enemy-rear battlefield, and psychological warfare battlefield." Some of these preparations must be done in a war's initial or preparation stage to ensure that no chance to strike is lost. Mao Zedong's statement about not practicing any idiotic humanity was then repeated by the author.[83]

Simple preparations helped to thwart or at least complicate some NATO IW missions according to other Chinese authors. These preparations included, according to one source, a French officer from the Kosovo Organization for Security and Cooperation in Europe who gave the Serbian armed forces part of NATO's attack plan; military experts sent to Iraq to learn from the Iraqis how to fight against NATO and U.S. planes (radar signatures, flight patterns, etc.); and drills and rehearsals teaching how to intercept cruise missiles.[84] Camouflaging key positions and equipment, and building false targets (burnt out armored vehicles with cut off telephone poles for main turrets, fake communications simulating command and control points, etc.) and false positions (bridges, etc.) caused NATO to waste assets on the wrong targets.

An interesting training article with a Kosovo IW twist also appeared in the Chinese press. The article was a summary of the first all-army collective training session for division and brigade chiefs of staff. Conducted by the Communications Command Academy, the instructors used the war in Kosovo as a frame of reference (the conference was held on 13 July 1999, shortly after the end of the fighting). One officer, Liu Xinsheng, noted that there were really four steps to NATO's combat performance. First, NATO used information reconnaissance operations to

acquire precise intelligence information on strike targets. Second, NATO used hard weapons to destroy or paralyze command and control systems and air defense systems of the Yugoslav armed forces. Third, NATO used precision combat led by electronic warfare to attack various military, economic, transportation, energy, public opinion, and other targets. Finally, NATO carried out damage assessments using airborne and ground photography and observations to determine the next bombing targets and make corrections. Information operations permeated these processes, such as NATO carrying out information blockades.[85]

The Yugoslav armed forces hid their equipment well and used traditional tactics as a counter to NATO reconnaissance missions. To deal with precision weapons, the Serbs divided the whole into parts, combining action with waiting and actively constructing a ground battlefield in which they moved to avoid destruction. They also studied the performance characteristics of Tomahawk cruise missiles to look for performance vulnerabilities. Tactics included:

- Avoiding strikes: by not turning on air defense radars, they kept NATO planes from finding their targets.
- Hooking the fish: they used folded corrugated steel or other materials as a decoy for radar, misleading the attacking missiles and aircraft
- Hide and seek: they took advantage of the blind zones and dead angles in the operational orbits and dead space of NATO reconnaissance satellites
- Relay intercept: they mixed the deployment of radars with different modalities and used the cross-deployment of weapons with different ranges to lay ambushes along the attack routes, switching on radar suddenly, performing intercept by firepower at different levels, and concentrating the fire of the weapons. This tactic was based on the mixed formations of NATO weaponry and their multi-echelon attacks.[86]

Finally, the conflict over Kosovo convinced the PLA that it must use short-term solutions while modernizing. The goal of catching up with America in IW in the next two decades is not one filled with optimism, especially after watching the advanced performance of NATO weaponry. But there is a serious will to accomplish this goal, especially since building an information economy and a PLA IW capability go hand in hand. IW is not just simulations and precision weapons, but also hacking, electronic jamming and paralyzing, and conducting disinformation campaigns. A sub goal is to “wreak havoc on opponents’ digital archives.” Thus, the battle over Kosovo, from a Chinese point of view, actually helped to speed up PLA modernization.

IW Exercises

There have been several significant Chinese IW military exercises during the past three years. Each is important, for exercises explain the transition from theory to practice. The first “special” (meaning IW) PLA battle took place in October 1997. In the Shenyang Military Region a Group Army (GA) underwent a computer attack that paralyzed its systems.The GA countered with virus killing software, and the exercise was termed an “invasion and anti-invasion” event. This exercise involved the deployment of ground, logistics, medical, and air force units. As one observer noted:

> the speed of marking and mapping on the computer screens by the advisors was more than 20 times fasterthan the traditional manual methods, and accuracy was 100 percent [faster]. The computer network in the command unit was activating more than 100 terminals, connecting and commanding a fourth-degree campaign network...the commanders attention was not on the number of documents handled, but on whether the high-tech design was excellent. Their focus was not on whether the commanding procedures and soldiers movements were standardized, but on how much high technology was being applied to their strategies and operations.[87]

The Taiwan Central News Agency on 27 December published a report on the exercise, and accused the PLA of using the exercise to develop a computer-virus warfare capability.[88]

In 1998, the Chinese offered another example of high-technology battlefield prowess when it staged an integrated high-technology exercise in October that united several military regions around the country. The center of gravity of the exercise was the Beijing Military Region, where a joint defense warfare drill used a "military information superhighway" for the first time. It was described as an information network sub-system of the command automation system[89], composed of digital, dial, command net, and restricted channels. Other elements of the command automation system are the command

operations, audio and graphics process and control, and data encryption sub-systems. The exercise started on 20 October and was coordinated with several other regions. The superhighway transmitted graphics, characters, and audio data in addition to situation maps.[90]

The Lanzhou Military Region, which includes the Gobi Desert, most likely also participated, since they reported on 26 October (as did the Beijing Region) of having participated in a high-technology exercise that emphasized electronic confrontation.[91] The focus of their effort was on electronic reconnaissance and counter-reconnaissance, electronic interference and counter-interference, and electronic destruction and counter-destruction.[92] Earlier in October, the General Staff reported that it too had held an all-army high-technology training exercise to discuss and design training issues to meet the challenges of the worldwide military revolution. Fu Quanyou, chief of the General Staff, attended and presided over the training exercise. They viewed the training of the Shenyang Military Region,[93] which may also have been part of the exercise mentioned above.

In October 1999 the PLA conducted another IW exercise. Two army groups of the Beijing Military Region conducted a confrontation campaign on the computer network. Reconnaissance and counter reconnaissance, interference and counter-interference, blocking and counter-blocking, and air strikes and counter air strikes were practiced. Six categories were included in the software environment: resource sharing, command operations, situation displays, supplementary assessments, signal transmissions, and intelligence. A computer evaluation system analyzed the performance of the participants in a quantitative and qualitative manner. The Operation Department of the General Staff said this was the first time that a computer confrontation was conducted at the campaign level between a red army and a blue army.[94] Actual field operations of a similar nature (counter reconnaissance, etc.) were conducted

simultaneously in the Jinan Theater. The performance of the high tech weaponry was like that of a tiger with wings, according to one observer.[95] The force demonstrated new tactics of using live ammunition to hit enemy cruise missiles and computer technology to hit information networks, links and points.[96] Advantages to using such high tech tools, according to reporter Zhang Feng, is that it enables a near-real "war laboratory" experience. It improves the science and technology quality and strategic level of commanders and staff, helps to improve the capability of the trainee to command joint operations, and has a very high training quality and "benefit to cost" ratio.[97]

The number of IW exercises is growing in the PLA. In July of 2000, the Chengdu Military Region conducteda confrontational campaign exercise on the Internet. The three training tasks associated with the exercise included organizing and planning the campaign, striving for air and information control, and making and countering breakthroughs. Over 100 terminals were linked for the exercise.[98] Three weeks later the Guangzhou Military Region conducted a high tech exercise. An order to start controlling communications channels was sent out to the subordinate units. The regiment in question has "shouldered the major task of conducting information operations and giving electromagnetic wave support during future wars."[99]

Conclusions

This discussion covered IW theory with Chinese characteristics. What conclusions do we draw after this lengthy discussion, first about Chinese IW and then about recommendations for the U.S. armed forces?

There are several issues to highlight about IW theory with a Chinese flavor. First, Chinese military theorists have found a willing, relatively cheap, and malleable ally in IW, an ally that can enable China to catch up with the West in both strategic military and international status. These areas could lead China to play an important strategic deterrent role (or potential troublemaker) in the Asia-Pacific region in the future and to gradually emerge into an economic competitor worthy of close scrutiny.

Second, China has placed an unusual emphasis on the emerging role of new IW forces. These various groups include a net force (separate armed forces branch), a shock brigade of network warriors, information protection troops, an information corps, electronic police, and a united network People's War organ, among other units. The latter is worthy of the most focus by foreign analysts due to its unique nature and potential. Interestingly, Western nations are currently the most capable of instituting such a concept, since computers reside in so many homes and offices, but the concept of forming an army from society is absent in these countries. Chinese theorists believe that an IW victory will very likely be determined by the side mobilizing the most computer experts to participate in take home battle. These forces would employ a strategy such as net point warfare, attempting to take out important information nodes and junctions. The Chinese believe in the power of network stability, and focus much of their IW theory on the protection of the network.

Third, Chinese IW emphasis currently reflects a mixture of Western and Chinese thinking that is moving away from the former. It is a Chinese proclivity to stress control, computerized warfare,

network warfare, and knowledge warfare instead of information superiority and "system of systems" theories which have become the norm in the West. In many ways, Chinese thinking is closer to that of the Russians due to a common frame of reference (military art and the Marxist dialectic). There has also evolved a Chinese specific IW lexicon that is different from Russia and the West. It includes such terms as acupuncture warfare, military soft science,[100] and informationized army

Fourth, Chinese IW often looks to Chinese military history to find answers to today's problems. These answers can be found in such rich locations as the secret art of war's 36 stratagems. The nature and characteristics of IW appear to fit well with these stratagems. Americans spend precious little time on such endeavors. On the other hand, China recognizes the capabilities inherent in Western IW and will think twice before engaging high tech opponents capable of winning in strategy with battle. However, the PLA was very impressed with Serbia's ability to withstand NATO's air attack. It demonstrated the power of the will of the people to the Chinese leadership and buttressed their belief in the power and capabilities of a People's War, a theory that now has a high technology application.

There are also plenty of weaknesses in the Chinese approach to IW, more than the number of strengths at the present time. This paper tried to highlight strengths and ways Chinese thinking differs from U.S. thinking. But the cornerstone of IW's operational theory involves preserving the integrity and stability of the infrastructure of one's side to perform IW functions. Infrastructure stability is as important as the survivability of units in the information age. And it is in the infrastructure where China's biggest weakness can be found. They are increasing their telecommunications industry rapidly, however, and laying a joint civil-military information infrastructure. China has been able to learn from the mistakes of others, and may soon become an IW force with which to reckon. IW has allowed China to skip over some technological developments, to use discoveries in the West to save time and money or to "borrow a ladder to climb the tree."[101] In addition, some Chinese theorists believe that to stray too far from the accepted definition of IW worldwide will not help China discuss the issues with other nations. But in the end, China will develop innovative, indirect IW strategies that do not imitate the moves of others. The important point to note is that it will be an IW force very different from other IW forces in the world.

Regarding the impact of Chinese IW theory and practice on U.S. armed forces, there are also several important points for consideration. First, the Chinese approach to information operations is dictated by the logic of the dialectic, the living interaction of point and counterpoint [thesis and antithesis] that inevitably produces a synthesis.The dialectical approach offers a unique way of visualizing and accounting for the use or misuse of information technologies and weapons. To understand this approach, America should train some of its specialists to think and analyze problems in this manner. Since Russia is also an adherent of the dialectic, two birds can be killed with one stone.

Second, the increased sophistication of the Chinese approach (knowledge warfare, temporal-spatial analysis, etc.) and emphasis on diverse aspects (confrontation of command and control, belief and perception systems, etc.) of IW cover areas scarcely ever discussed by U.S. analysts. This is particularly true for the multifaceted aspects of military art and important subsets such as

the 36 stratagems of war, as just one example. Study of the Chinese context and military strategies for information warfare may help avoid or deter future conflict by exposing areas of potential tension, misunderstanding, or even overt aggressiveness.Finally, study of the Chinese approach may assist U.S. policy makers in better understanding Chinese policy in other military-political realms.This understanding could range from Chinese responses to Russian IW declarations presented to the United Nations, or to the strategic context for any potential conflict with Taiwan.

There are other IW areas in which China, like Russia, can be expected to excel during the coming decade.From a purely academic point of view, China possesses a wealth of scientists and technicians who specialize in engineering and mathematical subjects that collectively form the intellectual basis for conducting information warfare.By function, the mathematicians can focus on preparing the algorithms necessary to produce sound software programs, and the academicians and theoreticians can develop innovative approaches to the study of information warfare by means of their dialectical thought process.Traditionally, just as they excel at the complex game of "go," the Chinese excel in the formulation of strategic concepts to include long term thought processes of point and counterpoint or anticipated challenge and response. Those subjects receive less attention among societies that are increasingly convinced of the inevitability of lasting peace.

In addition, Chinese specialists are devoting enormous efforts to "soft" or "asymmetric" approaches to confuse or thwart the potential information warfare threat that China envisions from abroad.This search is currently focusing on methods for influencing command and control apparatuses and various anti-reconnaissance and anti-cruise missile tactics.This emphasis was clearly evident in the Chinese analysis of the Kosovo crisis. The ability of the Serbs to maintain the mobility of their air defense weapons and to turn their radars on and off abruptly and for short periods was the sort of asymmetric response that sharply reduced potential Serb losses to attacking NATO forces.

The Chinese military is also gradually accumulating expertise in their study of the impact of information warfare on military art and what has come to be known as the cognitive aspect of information warfare. Chinese military scientists have studied the ability of information warfare to affect the values, emotions, and beliefs of target audiences, traditional psychological warfare theory, but with IW applications.

Thus, for the U.S. military, a force focused on information superiority, dominant maneuver, digitalization, and information assurance, a study of Chinese IW methods would be not only advisable but required. Such a study might uncover inherent IW weaknesses in the U.S. system when analyzed through the thought process of another ideological prism or framework. The absolute worse mistake that America can make is to use its own process for uncovering vulnerabilities exclusively, since there are other problem-solving schemes (the dialectic) available. As the Chinese have said, losers in IW will not just be those with backward technology. They will also be those who lack command thinking and the ability to apply strategies. It is worth the time of the U.S. analytical community to analyze IW strategies and tactics from all points of view, not just the empirical U.S. approach.

ENDNOTES

[1]The author does not speak Chinese. He relied on translations from the Foreign Broadcast Information System (FBIS) and on personal interviews conducted with the assistance of a translator while in China. For articles on Chinese IW written by Chinese language and subject matter experts, see the excellent work ofJames Mulvenon and Michael Pillsbury in particular.

[2]The cornerstone of IW's operational theory, to some Chinese theorists, involves preserving the integrity and stability of the infrastructure of one's side to perform these functions. Infrastructure stability is more important than survivability of units. See Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands," Beijing Jiefangjun Bao, 3 March 1998, p. 6 as translated and downloaded from the FBIS web site on 16 March 1998.

[3] Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to research in IW," Jiefangjun Bao, 7 November 1995, p. 6 as translated and reported in FBIS-CHI-95-239, 13 December 1995, pp. 22-27.

[4]Wang and Lin, "Viewing our Army's Quality…"

[5]Bill Gertz, "Hackers Linked to China Stole Documents from Los Alamos," The Washington Times, 3 August 2000, p. 1.

[6] Wang and Lin.

[7] Shen Weiguang, "Checking Information Warfare-Epoch Mission of Intellectual Military," Jiefangjun Bao, 2 February 1999, p. 6 as translated and downloaded from the FBIS web site on 17 February 1999.

[8]Li Yinnina, in Huang Youfu, Zhang Bibo, and Hang Song, "New Subjects of Study Brought about by Information War—Summary of Army Command Academy Seminar on 'Confrontation of Command' on the Information Battlefield" Jiefangjun Bao, 11 November 1997, p. 6 as translated and reported in FBIS-CHI-97-354, insert date 23 December 1997.

[9] Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," Kuang Chiao Ching (Hong Kong), 16 January, 1996, No. 280, pp. 22, 23 as translated and published by FBIS-CHI-96-035, 21 February 1996, pp. 33, 34.

[10]Wang Pufeng, "Meeting the Challenge of Information Warfare," Zhongguo Junshi Kexue (China Military Science), 20 February 1995, No 1, pp. 8-18 as translated and reported in FBIS-CHI-95-129, 6 July 1995, pp. 29, 30.

[11]Wei Jincheng, "New Form of People's Warfare," Jiefangjun Bao, 11 June 1996, p. 6 as translated and reported in FBIS-CHI-96-159, insert date 16 August 1996.

[12] Shen, "Focus of Contemporary World Military Revolution…".

[13]Wang Xiaodong, "Special Means of Warfare in the Information Age: Strategic Information Warfare," Jianchuan Zhishi, 30 June 1999 as translated and downloaded from the FBIS web site on 27 July 1999.

[14]Shen, "Checking Information Warfare…"

[15]Yang Shuqi and Guo Ruobing, [no title provided], Beijing Zhongguo Guofang Keji X, September-December 1996, No 5/6, pp. 90-93 as translated and reported in FBIS-CHI-98-029, insert date 30 January 1998.

[16]Ibid.

[17]China National Defense News, 24 January 2000, provided by Mr. William Belk via e-mail. Mr. Belk is the head of a skilled U.S. reservist group that studies China.

[18]Xu Jiwu and Xiao Xinmin, "Civil Networks Used in War," Beijing Jiefangjun Bao (Internet version-www) in Chinese, 1 July 2000, p. 2 as translated and downloaded by FBIS on 3 July 2000.

[19]China National Defense News, 15 December 1999, p. 1, provided by Mr. Belk via e-mail.

[20]Qianjin Bao, 10 December 1999, provided by Mr. Belk via e-mail..

[21]China National Defense News, 26 January 2000, provided by Mr. Belk via e-mail.

[22]"PRC Army Pays Attention to the Role of Network Warfare," Hong Kong Zhongguo Tonnxun She, 0947 GMT, 6 August 2000, as translated and downloaded from the FBIS web site on 6 August 2000.

[23]These strategies and their meanings were downloaded from http://www.chinastrategies.com, while the information age interpretation is from the author of this work.

[24] Qi Jianguo, "Thought on Internet War," Beijing Jiefangjun Bao, Internet version, 16 May 2000, p. 6 as translated and downloaded from the FBIS web site on 16 May 2000.

[25]Zhang Guoyu, "Symposium on Challenge of Knowledge Revolution for the Military," Jiefangjun Bao, 5 January 1999, p. 6 as translated and downloaded from the FBIS web site on 27 January 1999.

[26] Shen, "Focus of Contemporary World Military Revolution…"

[27] Li Yinnina, in Huang Youfu, Zhang Bibo, and Hang Song, "New Subjects of Study…"

[28] Cui Yonggui, in Zhang Guoyu's "Symposium on Challenge of Knowledge Revolution for the Military," Jiefangjun Bao, 5 January 1999, p. 6 as translated and downloaded from the FBIS website on 27 January 1999.

[29]Leng Bingling, Wang Yulin, and Zhao Wenxiang, "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power," Beijing Jiefangjun Bao, 11 November 1997, p. 7 as translated and downloaded from the FBIS web site on 11 November 1999.

[30]Ibid.

[31]Shen,"Focus of Contemporary World Military Revolution…"

[32]Hai and Chang, "Chinese Military Studies Information Warfare"

[33]Wang Huying, "Exploring and Analyzing Characteristics of Information Warfare," Jiefangjun Bao, 30 January 1996, p. 6 as translated and reported in FBIS-CHI-96-030, 13 February 1996, pp. 21, 22.

[34]Su Enze, "Logical Concept of Information Warfare," Jiefangjun Bao, 11 June 1996, p. 6 as translated and reported in FBIS-CHI-96-135, insert date 15 July 1996.

[35] Shen,"Checking Information Warfare…"

[36]Wang Baocun, "New Military Revolution in the World, 'Subduing Enemy Force without Battle' and Informationized Warfare," Zhongguo Junshi Kexue, 4 May 1999, pp. 60-63 as translated and downloaded from the FBIS web site on 23 August 1999.

[37]Joint Pub 3-13, Joint Doctrine for Information Operations, 9 October 1998, p. I-9.

[38]Ibid., p. I-11.

[39]Shen Weiguang, [no title provided], Beijing Zhongguo Guofang Keji X, September-December 1996, No 5/6, pp. 87-89 as translated and reported in FBIS-CHI-98-029, insert date 30 January 1998.

[40]Yang and Guo, [no title provided]

[41]Liang Zhexing, [no title provided], Beijing Zhongguo Dianzi Bao [China Electronics News], speech presented 15 September 1997 but printed on 24 October 1998, as translated and reported in FBIS-CHI-98-012, insert date 13 January 1998.

[42]Wang Baocun, "A Preliminary Analysis of IW," Beijing Zhongguo Junshi Kexue, No 4, 20 November 1997, pp 102-111 as translated and downloaded from the FBIS web site on 20 November 1997,

[43]Wang and Lin, “Viewing Our Army’s Quality…”

[44] Shen, “Checking Information Warfare…”

[45]Yuan Banggen, “On IW, Digital Battlefields,” Beijing Zhongguo Junshi Kexue, 20 February 1999, pp. 46-51 as translated and downloaded from the FBIS web site on 17 July 1999.

[46]Wang, “New Military Revolution…”

[47]Xie Guang,” Wars under High Tech,” Beijing Renmin Ribao, 27 December 1999, p. 7 as translated and downloaded from the FBIS web page on 30 January 1999.

[48]Wang Pufeng, [no title provided], Hong Kong Hsien-Tai Chun-Shih (Conmilit), 11 April 2000, pp. 19-21 as translated and downloaded from the FBIS web site on 3 May 2000.

[49]Yuan, “On IW, Digital Battlefields,”.

[50]Ibid.

[51]Ibid.

[52]Cui Yonggui, in Zhang Guoyu’s “Symposium on Challenge of Knowledge Revolution for the Military,” Jiefangjun Bao, 5 January 1999, p. 6 as translated and downloaded from the FBIS website on 27 January 1999.

[53]Qi Jianguo, “Thought on Internet War,” Beijing Jiefangjun Bao, Internet version, 16 May 2000, p. 6 as translated and downloaded from the FBIS web site on 16 May 2000.

[54]Ibid.

[55] Shen, [no title provided]

[56]Wang, “New Military Revolution…”

[57]Yang Minqing, “Facing the Future Information War,” Jingji Cankao Bao, 15 October 1999, p. 5 as translated and downloaded from the FBIS web site on 29 November 1999.

[58]Lei Yuanshen, “New Breakthrough in the Study of Information Warfare,” Jiefangjun Bao, 21 July 1998 p. 6 as translated and downloaded from the FBIS web site on 12 August 1998.

[59]“Chinese Military Holds Training Course on Information War,” Beijing Xinhua, 22 May 2000 as translated and downloaded from the FBIS web site on 22 May 2000.

[60]“University to Foster Talent for High-Tech Warfare,” Xinhua, 17 November 1999 as translated and downloaded from the FBIS web site on 17 November 1999.

[61]Ma Xiaochun, “PLA Sets Up Four New Academies,” Beijing Xinhua, 2 July 1999 as translated and downloaded from the FBIS web site on 7 July 1999.

[62]“PLA Trains Personnel for Information Warfare,” Hong Kong Tai Yang Pao 15 September 1999, p. A17 as translated and downloaded from the FBIS web site on 15 September 1999.

[63]Guo Hao, “Chinese Military Prepares to Fight Digital Warfare,” Kong Kong Kuang Chiao Ching, 16 March, 2000, No 330 pp 19-21 as translated and downloaded from the FBIS web site on 16 March 2000.

[64]Xi Qixin and Zhao Yongxin, “Advancing Toward High Technology—High Ranking Military Cadres Attending a Hi-Tech Training Course,” Xinhua Domestic Service, 13 June 1999 as translated and downloaded from the FBIS web site on 15 June 1999.

[65] Zhang Zhenzhong and Chang Jianguo, “Train Talented People at Different Levels for Information Warfare,” Jiefangjun Bao, 2 February 1999 p. 6 as translated and downloaded from the FBIS web site on 10 February 1999.

[66]Wang Wowen, “PRC Senior Military Cadres Trained on High Technology,” Xinhua Domestic Service, 11 April 2000 as translated and downloaded from the FBIS web site on 11 April 2000.

[67]“Shao Zijun Says the Navy Engineering College is Aimed at Developing New Naval Military Talent,”Xinhua Hong Kong, 7 August 1999 as translated and downloaded from the FBIS web site on 26 August 1999.

[68]Lei Zhuomin, “Information Warfare and Training of Skilled Commanders,” Jiefangun Bao, 26 December 1995 p. 6 as translated in FBIS document FBIS-CHI-96-036, 26 December 1995.

[69]Cheng Bingwen, “Let Training Lean Close to Information Warfare,” Jiefangjun Bao, 12 November 1996 p. 6 as translated and reported in FBIS-CHI-96-230, inserted on 29 November 1996.

[70]Zhang and Chang, “Train Talented People…”

[71]Ibid.

[72]Ibid.

[73]Ibid.

[74]Sun Haicheng, Yang Jie, and Zhang Guoyu, “Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory,” Jiefangjun Bao, 13 July 1999 p. 6 as translated and downloaded from the FBIS web site on 8 August 1999.

[75]Mao Xiaochun and Chen Hui, “Chief of Staff Fu Quanyuou on High-tech Military Training,” Xinhua Domestic Service, 0240 GMT, 16 October 1999 as translated and downloaded from the FBIS web site on 16 October 1999.

[76]Fan Changlong, “Stand in the Forefront of the New Military Revolution in Deepening Troop training through Science and Technology,” Jiefangjun Bao, 4 April 2000 p. 6 as translated and downloaded from the FBIS web site on 6 April 2000.

[77]Wang Baocun, “Information Warfare in the Kosovo Conflict,” Beijing Jiefangjun Bao, 25 May 1999,p. 6 as translated and downloaded from the FBIS web site on 23 June 1999.

[78]Ibid.

[79]“Military Forum” page, The Liberation Army Daily, 27 July 1999, report obtained via e-mail from Mr. William Belk,1 June 2000.

[80]Wang, “Information Warfare in the Kosovo Conflict”

[81]Su Size, “Kosovo War and New Military Theory,” Beijing Jiefangjun Bao, 1 June 1996, as translated and downloaded from the FBIS web page on 1 July 1999.

[82] Jia Weidong, “Asymmetrical War and Smart War—The Developing Trends of Future War from a Kosovo Perspective,” Beijing Jiefangjun Bao, 17 April 1999, p. 6 as translated and downloaded from the FBIS web site on 10 May 1999.

[83]Zhu Xiaoning, “A Monopoly on the Asymmetrical Battlefield,” Beijing Jiefangjun Bao,23 November 1999, p. 6 as translated and downloaded from the FBIS web site on 26 December 1999.

[84]Beijing Xinhua Hong Kong Service, 0527 GMT 24 May 1999 as translated and downloaded from the FBIS web page on 26 May 1999.

[85] Sun, Yang, and Zhang, “Let Information Warfare Training Rule…”

[86]Ibid.

[87]Beijing Xinhua, 1508 GMT, 22 October 1997, as downloaded in translated form from the FBIS WebPages.

[88]Taiwan Central News, 1057 GMT, 27 December 1997, as downloaded in translated form from the FBIS WebPages.

[89]In July 1999 the Theater of Operations stated that it had built the first theater command automation system. The system combines command, control, intelligence, communications countermeasures and joint command and management functions to allow ground, naval and air forces to share information at the theater, army, division, and regimental levels. This “God of

Field Operations" reportedly combines information processing with data facsimile, terminal processing, and GPS imaging. See "Guangzhou Theater of Operation Builds Army's First Command Automation System,"Beijing Zhongguo Xinwen She, 26 July 1999 as translated and downloaded from the FBIS web page on 10 August 1999.

[90]Beijing Xinhua Domestic Service, 1148 GMT, 26 October 1998, as translated and downloaded from the FBIS web page.

[91]Ren Yanjun and Zhang Jianjun, "General Staff Department Holds All-Army Hi-Tech Training Exercise," Beijing Jiefangjun Bao, 2 October 1998, p. 1 as translated and downloaded from the FBIS web pages.

[92]Beijing Zhongguo Xinwen She, 1309 GMT, 26 October 1998, as translated and downloaded from the FBIS web page on 3 November 1998.

[93]Ibid.

[94]Yang Hong and Zhou Meng, "Beijing Military Region Conducts Computer Exercise," Beijing Jiefangjun Bao, Internet version, 8 November 1999, as translated and downloaded from the FBIS web site on 9 November 1999.

[95]Beijing Zhongguo Xinwen She, 1339 GMT, 6 November 1999, as translated and downloaded from the FBIS web site on 9 November 1999.

[96]Beijing Xinhua Domestic Service, 0905 GMT, 15 October 1999 as translated and downloaded from the FBIS web site on 15 October 1999.

[97]Zhang Feng, "The Chinese Armed Forces Advance toward the Virtual Battlefield…" Beijing Jiefangjun Bao, 24 November 1999, p. 5 as translated and downloaded from the FBIS web site on 24 November 1999.

[98]Xu Wenliang and Wan Yuan, "Chengdu Military Region Conducts Long-Range Confrontational Exercises on Internet," Beijing Jiefangjun Bao, Internet version, 10 July 2000 as translated and downloaded from the FBIS web site on 10 July 2000.

[99]Yang Quansheng, Zhang Shusong, and Wang Yongqing, "Guangzhou Military Region Regiment Steps Up Capability to Fight Information Warfare," Beijing Jiefangjun Bao, Internet version, 31 July 2000, p. 2 as translated and downloaded from the FBIS web site on 31 July 2000.

[100]Shen, "Focus of Contemporary…"

[101]Wang and Lin, "Viewing Our Army's…"